福井大学
工学部　研究報告
第46巻　第2号
1998年9月

離散対数生成器に基づく楕円曲線暗号系

王 尚平*　西野 順二**　小高 知宏**　小倉 久和**

Elliptic Curve Cryptosystem on the Base of Discrete Logarithm Generator

Shangping WANG, Junji NISHINO, Tomohiro ODAKA and Hisakazu OGURA

(Received Aug. 29, 1998)

In this paper, we showed the theory of elliptic curve, discrete logarithm problem (DLD), elliptic curve discrete logarithm problem (EDLP), discrete logarithm generator and ElGamal cryptosystem and elliptic cryptosystem. After that work, we proposed an elliptic curve cryptosystem on the base of discrete logarithm generator. The security of the proposed cryptosystem depend on the intractability of EDLP. At present no one seems to have a subexponential time algorithm for EDLP. So the proposed cryptosystem have the sufficient security.

Key Words: Cryptosystem, Elliptic Curve, EDLP, Discrete Logarithm Generator, Public Key

1　はじめに

秘密鍵暗号系（private key cryptosystem）では暗号化鍵が復号鍵と同じである．秘密鍵暗号系の欠点は，暗号文を送る前に，送信者と受信者の間で安全な通信路を使って鍵Kをあらかじめ送信することが要求されることである．実際問題として，これを実現するのは非常に困難である．公開鍵暗号系（public key cryptosystem）とは暗号化鍵と復号鍵が異なる暗号系である．つまり，暗号化鍵E_kから復号鍵D_kを求めることが計算量的に困難な暗号系である．公開鍵暗号系の考えは，1976年にDifferとHellman[1]とによって発案された．公開鍵暗号系では，各ユーザーが暗号化鍵と復号鍵を一対ずつ作成し，各ユーザは自分の暗号鍵（公開鍵）を電話帳のように公開し復号鍵（秘密鍵）を秘密に保持することにより，自分の秘密鍵さえ管理しておけば誰とでも暗号通信ができる．これは公開鍵暗号系の利点である，しかし公開鍵暗号系の効率性は秘密鍵暗号系のそれより低い．実際に公開鍵暗号を運用する際には，送信者は受信者が公開した暗号化鍵を用いて平文を暗号文に変換するのである．受信者は秘密にしている復号鍵

*大学院情報工学専攻
**情報工学科

を用いて復号する．復号鍵が他の人に知られていなければ，受信者がその暗号文を復号できる唯一の人物である．従って，鍵配送の必要がない．公開鍵暗号系のもう一つ利点はディジタル署名が可能なことである．ディジタル署名は文書の署名、捺印に相当する．従ってビジネスの上での争いを避けるためにはディジタル署名は必要不可欠である．

楕円曲線理論は，整数論において研究されていた分野である．しかしながら，最近楕円曲線は暗号の分野で脚光をあびている．これが楕円曲線暗号系である．楕円曲線暗号系は公開鍵暗号系の一種で，現在知られている公開鍵暗号系の中で，1ビットあたりの安全性が最も高い．離散対数生成器は離散対数問題に基づく疑似乱数生成器（pseudo-random bit generator，PRBG）である．PRBGはシード（seed）と呼ばれる短いランダムビット列をより長いランダムビット列に伸ばすものである．本研究では離散対数生成器と楕円曲線理論を融合した，離散対数生成器に基づく楕円曲線暗号系を提案する．

2 楕円曲線と離散対数問題

2.1 楕円曲線

任意の体 K の上の楕円曲線は

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in K \tag{1}$$

で与えられる．体 K の標数が2あるいは3でない場合は次のように簡単な形で与えられる．

$$y^2 = x^3 + ax + b \qquad a, b \in K \tag{2}$$

ここで，a, b は $4a^3 + 27b^2 \neq 0$ である．楕円曲線 $E(K)$ は(2)を満たす点 $(x, y) \in K^2$ の集合であるが，$x \to \infty$ のとき $y \to \infty$ と考えて，無限遠点 $O = (\infty, \infty)$ も楕円曲線の点と考える．

標数が2あるいは3でない有限体 $F(p)$ 上の楕円曲線 $E(F_p)$ は加法を次のように定義するとアーベル群 (Abelian group) となる．ただし，すべての算術演算は $F(p)$ 上で行なう．

$P = (x_1, y_1), Q = (x_2, y_2)$ を $E(F_p)$ 上の点として．和 $P + Q$ を，

$x_1 = x_2$，$y_2 = -y_1$ならば，　$P + Q = O$ (3)

そうでないならば，　$P + Q = (x_3, y_3)$ (4)

となる．ただし，

$$x_3 = s^2 - x_1 - x_2 \tag{5}$$

$$y_3 = s(x_1 - x_3) - y_1 \tag{6}$$

$$s = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & ,if \quad P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & ,if \quad P = Q \end{cases} \tag{7}$$

である．Oが加法の零元で，任意の $P = (x, y) \in E(F_p)$ 対し，

$$P + O = O + P = P \tag{8}$$

となることは，以上の定義より容易に示せる．また，$P = (x, y)$ の逆元 $-P = -(x, y)$ は

$$-(x, y) = (x, -y) \tag{9}$$

と表せる．Pの倍数は，$2P = P + P$，$3P = 2P + P$などと定義する．

有限体 $F(p)$ 上の楕円曲線 $E(F_p)$ 上の点の数$\#E(F_p)$ は $Hasse$ の定理 [2] より

$$p + 1 - 2\sqrt{p} \leq \#E(F_p) \leq p + 1 + 2\sqrt{p} \tag{10}$$

となる．楕円曲線 $E(F_p)$ 上の点 Pに対して，常に

$$(\#E(F_p))\,P = O \tag{11}$$

の関係が成立する．一般に，楕円曲線 $E(F_p)$ 上の点 Pに対して

$$mP = O \tag{12}$$

が成立する最小の整数 m を Pの位数という．ある点 $G \in E(F_p)$ の位数が$\#E(F_p)$ であるとき，G を $E(F_p)$ の原始元と呼ぶ．$E(F_p)$ の異なる原始元の数は，φ をオイラー関数として $\varphi(\#E(F_p))$で与えられる．

例えば，$a = 2, b = 5, p = 47$ のとき，楕円曲線 $y^2 \equiv x^3 + 2x + 5 \bmod 47$ の解(x, y)全体の集合 $E(F_{47})$ は以下のようになる
(1,14), (1,33), (2,8), (2,39), (8,4), (8,43), (9,0), (11,18), (11,29), (12,21), (12,26), (14,2), (14,45), (17,8), (17,39), (20,14), (20,33), (21,7), (21,40), (22,13), (22,34), (24,23), (24,24), (26,14), (26,33), (27,7), (27,40), (28,8), (28,39), (29,23), (29,24), (33,10), (33,37), (40,20), (40,27), (41,23), (41,24), (43,11), (43,36), (46,7), (46,40), (∞, ∞)

$E(F_{47})$ 上の点の数は$\#E(F_{47}) = 42$ であり，点 (2,8) の位数は 6，点 (1,14) の位数は 42 である．これより点 (1,14) は $E(F_{47})$ の原始元である．$E(F_{47})$ の異なる原始元の数は$\varphi(\#E(F_{47})) = \varphi(42) = (2-1)(3-1)(7-1) = 12$ である．

2.2 離散対数問題

G を演算$\odot$とする有限群として，ある$\alpha \in G$ に対し，$H = \{\alpha^i : i \geq 0\}$ をαが生成する G の部分群（巡回群）であるとする．$\alpha \in G$，$\beta \in H$があたえられたとき

$$\beta = \alpha^x = \underbrace{\alpha \odot \cdots \odot \alpha}_{x\text{回}} \tag{13}$$

となる x $(0 \leq x \leq |H| - 1)$を求める問題を離散対数問題（discrete logarithm problem , DLP）と呼ぶ．この x を $\log_\alpha \beta$と書く．同様に $F(p)$ 上の楕円曲線 $E(F_p)$ 上の点 $Y, Z \in E(F_p)$ とがあたえられたとき

$$Y = xZ = \underbrace{Z + \cdots + Z}_{x\text{回}} \tag{14}$$

となる x が存在するならばその x を求める問題を楕円曲線上の離散対数問題（elliptic curve discrete logarithm problem，EDLP）と呼ぶ．

離散対数問題と楕円曲線上の離散対数問題は計算量的に困難な問題である（4.3 節参照）．現在，離散対数問題と楕円曲線上の離散対数問題は公開鍵暗号系への応用で注目されている．

3 楕円曲線を用いた ElGamal 暗号系と Menezes-Vanstone 暗号系

3.1 ElGamal 暗号系

ElGamal 暗号系 [3] は離散対数問題に基づいた公開鍵暗号系である．この ElGamal 暗号系は次の通りである．

> p を体 F_pにおいて離散対数問題が手に負えなくなる素数とし，また，F_p^*を，$\alpha \in F_p^*$を原始元とする乗法群であるとする．

受信者 B の公開鍵：素数 p，F_p^*の原始元α，および$\beta(\equiv \alpha^a \bmod p)$.
受信者 B の秘密鍵：a $(1 < a < p-1)$
送信者 A が受信者 B に平文 $x \in F_p^*$を送りたいとする.
送信者 A の暗号化：A は乱数 kを発生し，次の式によって，平文 x の暗号文 (y_1, y_2) を得る．ただし，$1 < k < p-1$ である.

$$y_1 = \alpha^k \bmod p \tag{15}$$
$$y_2 = x\beta^k \bmod p \tag{16}$$

送信者 A は受信者 B に平文 x の暗号文 (y_1, y_2) を送る.
受信者 B の復号：受信者 B は受け取った暗号文 $y_1, y_2 \in F_p^*$に対して，自分の秘密鍵 a を用いて，次の式によって，平文 x を復号できる.

$$y_2(y_1^a)^{-1} \bmod p = x \tag{17}$$

ElGamal 暗号系は，暗号文が平文 x と乱数 kに依存しており，非決定的である．よって，一つの平文からいろいろな暗号文が生成される.

明らかに ElGamal 暗号系のシステム安全性は離散対数問題に基づいたもので，$a = \log_\alpha \beta$を求めるのが計算量的に困難であることに依存している．また，楕円曲線上の離散対数問題に基づいた ElGmal 暗号系を構成することができ，楕円曲線暗号系（楕円曲線を用いた ElGamal 暗号系）[4] と呼ばれる．楕円曲線暗号系は次の通りである．

楕円曲線を $E(F_p)$：$y^2 \equiv x^3 + ax + b \bmod p$ とする．また，$\alpha = (x_0, y_0) \in E(F_p)$ を楕円曲線 $E(F_p)$ の原始元とする.
受信者 B の公開鍵 ：$\alpha = (x_0, y_0) \in E(F_p)$ と $\beta(= d\alpha)$
受信者 B の秘密鍵 ：d (d は整数)
送信者 A が受信者 B にメッセージ $x \in E(F_p)$ を送りたいとする.
送信者 A の暗号化：送信者 A は乱数 kを発生し，平文 x の暗号文 (c_1, c_2)を次の式で計算する.

$$c_1 = k\alpha \tag{18}$$
$$c_2 = x + k\beta \tag{19}$$

受信者 B の復号：受信者 B は受け取った (c_1, c_2)から，自分の秘密鍵 d を用いて，次のように復号する.

$$x = c_2 - dc_1 \tag{20}$$

実際，式 (20) おいて，$c_2 - dc_1 = (x + k\beta) - d(k\alpha) = x + k(d\alpha) - d(k\alpha) = x$ となり，復号できている.

例えば 2.1 節の例では，受信者 B の公開鍵を $\alpha = (x_0, y_0) = (1, 14)$ と$\beta(= d\alpha) = (21, 7)$，秘密鍵を $d = 28$ として次のように暗号通信を行う.
送信者 A が受信者 B にメッセージ $x = (26, 33) \in E(F_{47})$ を送りたいとする.
送信者 A の暗号化：送信者 A は乱数 $k = 32$ を発生し，式 (18) (19) によって

$$c_1 = k\alpha = 32(1, 14) = (27, 7)$$
$$c_2 = x + k\beta = (26, 33) + 32(21, 7) = (26, 33) + (21, 40) = (17, 39)$$

として，x の暗号文 $(c_1, c_2) = ((27,7),(17,39))$ 得る．送信者 A が受信者 B に暗号文 $(c_1, c_2) = ((27,7),(17,39))$ を送る．

受信者 B の復号：式 (20) によって，平文 $x = (26,33)$ を復号できる．

$$x = c_2 - dc_1 = (17,39) - 28(27,7) = (26,33)$$

3.2 Menezes-Vanstone 楕円曲線暗号系

楕円曲線暗号系では，送信者 A が受信者 B にメッセージ x を送りたいとするとき，x は，$x \in E(F_p)$ でなければならない．もしメッセージ $x = (x_1, x_2)$ が楕円曲線 $E(F_p)$ 上の点でないときには，楕円曲線暗号系は使うできない．これに対して，Menezes-Vanstone 楕円曲線暗号系 [5] が提案されている．

受信者 B の公開鍵：$\alpha = (x_0, y_0) \in E(F_p)$ と $\beta(= d\alpha)$

受信者 B の秘密鍵：d (d は整数)

送信者 A が受信者 B にメッセージ $x = (x_1, x_2) \in Z_p \times Z_p$ を送りたいとする．

送信者 A の暗号化：送信者 A は乱数 k を発生し，次の式によって x の暗号文 $y = (z, y_1, y_2)$ を得る．

$$z = k\alpha \tag{21}$$
$$(c_1, c_2) = k\beta \tag{22}$$
$$y_1 = c_1 x_1 \bmod p \tag{23}$$
$$y_2 = c_2 x_2 \bmod p \tag{24}$$

受信者 B の復号：受信者 B は受け取った暗号文 $y = (z, y_1, y_2)$ から，自分の秘密鍵 d を用いて，次のようにメッセージ $x = (x_1, x_2)$ を復号できる．

$$(c_1, c_2) = dz \tag{25}$$
$$x_1 = y_1 c_1^{-1} \bmod p \tag{26}$$
$$x_2 = y_2 c_2^{-1} \bmod p \tag{27}$$

式 (25) おいて，$dz = d(k\alpha) = k(d\alpha) = k\beta = (c_1, c_2)$ である．式 (26) (27) は式 (23) (24) によって成立している．

例えば 2.1 節の例で，メッセージを $x = (5,7)$ とすると，これは楕円曲線 $E(F_{47})$ 上の点ではない．これに対して，Menezes-Vanstone 楕円曲線暗号系を使う．

受信者 B の公開鍵：$\alpha = (x_0, y_0) = (1,14)$ と $\beta = d\alpha = (24,23)$

受信者 B の秘密鍵：$d = 25$

送信者 A の暗号化：A は乱数 $k = 17$ を発生し，式 (21) ～ (24) によって

$$z = k\alpha = 17(1,14) = (24,24)$$
$$(c_1, c_2) = k\beta = 17(24,23) = (22,13)$$
$$y_1 = c_1 x_1 \bmod p = 22 \times 5 \bmod 47 = 16$$
$$y_2 = c_2 x_2 \bmod p = 13 \times 7 \bmod 47 = 44$$

$x = (5,7)$ の暗号文 $y = (z, y_1, y_2) = ((24,24),16,44)$ が得られる．

受信者 B の復号：受信者 B は受け取った暗号文 $y = (z, y_1, y_2) = ((24,24),16,44)$ から，自分の秘密鍵 $d = 25$ を用いて，式 (25) ～ (27) によってメッセージ $x = (x_1, x_2) = (5,7)$ を復号できる．

$$dz = (c_1, c_2) = 25(24, 24) = (22, 13)$$
$$x_1 = y_1 c_1^{-1} \bmod p = 16(22)^{-1} \bmod 47 = 16 \cdot 15 \bmod 47 = 5$$
$$x_2 = y_2 c_2^{-1} \bmod p = 44(13)^{-1} \bmod 47 = 44 \cdot 29 \bmod 47 = 7$$

4 離散対数生成器に基づく楕円曲線暗号系の提案

4.1 離散対数生成器

疑似乱数生成器は短いランダムなビット列（シード）から，より長い乱数のようなビット列（疑似乱数列）を生成するアルゴリズムの機構をもつものである．このような疑似乱数生成器があれば，ランダムなシードからメッセージと同じ長さの疑似乱数を生成し，使い捨て鍵暗号のようにメッセージに作用させればよい．使い捨て鍵暗号（One-time pad）では，平文と鍵はともに特定の長さのビット列であり，暗号文は平文と鍵のビットごとの排他的理論和をとって構成される．離散対数生成器 [6] は離散対数問題に基づく PRBG である．この PRBG は次の通りである．

p を kビットの素数，$\gamma \in F_p^*$を原始元とする．ここで，F_p^*は乗法群である．シード x_0は F_p^*の任意の要素である．$i \geq 0$ に対して

$$x_{i+1} = \gamma^{x_i} \bmod p \tag{28}$$

と定義し，さらに

$$r_i = \begin{cases} 1 & ,if \quad x_i > p/2 \\ 0 & ,if \quad x_i < p/2 \end{cases} \tag{29}$$

としたうえで

$$f(x_0) = (r_1, r_2, \cdots, r_l) \tag{30}$$

と定義する．fは (k,l)-離散対数生成器（Discrete Logarithm Generator）とよばれる．

例えば，$p = 47$ を $k = 6$ ビットの素数として，$\gamma = 5 \in F_{47}^*$は原始元である．シード $x_0 = 16$ と $l = 32$ から，式（28）（29）によって，(6,32)-離散対数生成器（疑似乱数列）は $f(16) = (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$を生成する．

4.2 離散対数生成器に基づく楕円曲線暗号系の提案

離散対数生成器を用いた使い捨て鍵暗号系は秘密鍵暗号系として効率的である．本論文では，現在知られている公開鍵暗号系の中で，1ビットあたりの安全性が最も高い楕円曲線暗号系と，離散対数生成器を用いた使い捨て鍵暗号系とを融合した，離散対数生成器に基づく楕円曲線暗号系を提案する．提案する暗号系は次のように構成する．

受信者 B の公開鍵 ：楕円曲線 $E(F_p)$ の原始元$\alpha = (x_0, y_0)$ と$\beta \in E(F_p)$ $(\beta = d\alpha)$，および F_p^* の原始元$\gamma \in F_p^*$.
受信者 B の秘密鍵 ：d (d は整数)

送信者 A が受信者 B にメッセージ $m = m_1 \circ m_2 \circ \cdots \circ m_l$を送りたいとする．ここで $m_i \in \{0, 1\}$ $(i = 1, \cdots, l)$ である．$\circ$ は連接である．

送信者 A の暗号化 ：

step(1-1)　A は乱数（シード）$x_0 \in F_p^*$を発生し，離散対数生成器を用いて，式（28）（29）によって，疑似乱数列 $f(x_0) = (r_1, r_2, \cdots, r_l)$を生成し，次にメッセージ m の各 m_iに対して

$$c_i = r_i \oplus m_i \ (i = 1, \cdots, l) \tag{31}$$

からなる暗号文 $c = c_1 \circ c_2 \circ \cdots \circ c_l$を作成する．

step(1-2)　送信者 A は乱数 kを発生し，式（21）（22）によって，zと (c_1, c_2) を計算し，次の式によって

$$y_1 = c_1 x_0 \bmod p \tag{32}$$
$$y_2 = c_2 l \bmod p \tag{33}$$

(x_0, l)の暗号文 $y = (z, y_1, y_2)$ である．送信者 A は暗号文 $c = c_1 \circ c_2 \circ \cdots \circ c_l$と $y = (z, y_1, y_2)$ を受信者 B に送る．

受信者 B の復号 ：

step(2-1)　受信者 B は受け取った暗号文 $y = (z, y_1, y_2)$ から，自分の秘密鍵 d を用いて，式（25）によって (c_1, c_2) を得る．次の式によって(x_0, l)を得る．

$$x_0 = y_1 c_1^{-1} \bmod p \tag{34}$$
$$l = y_2 c_2^{-1} \bmod p \tag{35}$$

step(2-2)　受信者 B はシード x_0を用いて，式（28）（29）によって，疑似乱数列 $f(x_0) = (r_1, r_2, \cdots, r_l)$ を生成し，次の式により，メッセージ m を復元する．

$$m_i = r_i \oplus c_i \ (i = 1, \cdots, l) \tag{36}$$
$$m = m_1 \circ m_2 \circ \cdots \circ m_l \tag{37}$$

例えば，楕円曲線を $E(F_{47})$ とする．

受信者 B の公開鍵を楕円曲線 $E(F_{47})$ の原始元$\alpha = (x_0, y_0) = (1, 14)$ と$\beta(\ = d\alpha) = (21, 7)$，および F_{47}^*の原始元$\gamma = 5 \in F_{47}^*$とする．受信者 B の秘密鍵は $d = 28$ である．

送信者 A が受信者 B にメッセージ $m = 00010111100011000001000111010000$ を送りたいとする．ここで $l = 32$ である．

送信者 A の暗号化：step(1-1) によって，A は乱数（シード）$x_0 = 16$ と $l = 32$ から，疑似乱数列 $f(16) = (0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0)$を生成し，式（31）によって，暗号文 $c = 01010100000100110110000010101000$ を作成する．

step(1-2) によって，送信者 A は乱数 $k = 17$ を発生し，式（21）（22）によって，$z = (24, 24)$ と $(c_1, c_2) = (22, 13)$ を計算し，次に式（32）（33）によって y_1, y_2を求める．

$$y_1 = 22 \cdot 16 \bmod 47 \quad = 23$$
$$y_2 = 13 \cdot 32 \bmod 47 \quad = 40$$

送信者 A は暗号文 c と $y = (z, y_1, y_2) = ((24, 24), 23, 40)$ を受信者 B に送る．

受信者 B の復号：step(2-1) によって，受信者 B は自分の秘密鍵 $d = 28$ を用いて，式（25）によって $(c_1, c_2) = (22, 13)$ を得る．次に式（34）（35）によって$(x_0, l) = (16, 32)$を得る．

$$x_0 = 23 \cdot (22)^{-1} \bmod 47 \quad = 23 \cdot 15 \bmod 47 \quad = 16$$
$$l = 40 \cdot (13)^{-1} \bmod 47 \quad = 40 \cdot 29 \bmod 47 \quad = 32$$

step(2-2) によって，受信者 B はシード $x_0 = 16$ を用いて，式（28）（29）によって，$f(16)$ を生成し，式（36）（37）により，メッセージ $m = 00010111100011000001000111010000$ を復元できる．

4.3 離散対数生成器に基づく楕円曲線暗号系の安全性

離散対数生成器に基づく楕円曲線暗号系の安全性は DLP と EDLP が計算量的に困難な問題であることに依存する．文献 [7] によれば，DLP に対する計算アルゴリズムとして Shanks のアルゴリズムと Pohlig-Hellman アルゴリズム，および指数計算法（index calculus method）が提案されているが，指数計算法が最も効率的である．p を kビットからなる素数として，この指数計算法は DLP を求めるのに，$exp(O(k)^{1/3}(\ln k)^{2/3})$ オーダの時間（準指数時間）であることが示されている．しかし，EDLP に対しては，もし，$\#E(F_p)$ が少なくとも一つ大きい素因数をもつときには EDLP を求めるのにかかる時間は $exp(O(k))$（指数時間）である．従って，DLP と EDLP を解くのにかかる時間は多項式時間ではない．ゆえに DLP と EDLP は計算量的に困難な問題となる．現在，計算量の観点から EDLP は 160 ビット程度以上の大きさならば安全であるとされている [7].

4.4 離散対数生成器に基づく楕円曲線暗号系のディジタル署名

離散対数生成器に基づく楕円曲線暗号系のディジタル署名は普通の楕円曲線暗号系のディジタル署名の方法と大体同じである．それは次の通りである．

Pは楕円曲線 $E(F_p)$ 上の点であり，Pの位数（order）は素数 qである．つまり，qは $qP = O$となる最小の整数である．
送信者 A の公開鍵：$Q_a(Q_a = d_aP)$
送信者 A の秘密鍵：$d_a(1 < d_a < q-1)$
受信者 B の公開鍵：$Q_b(Q_b = d_bP)$
受信者 B の秘密鍵：$d_b(1 < d_b < q-1)$
送信者 A がメッセージ m にディジタル署名を行いたいとする．
step (3-1)　A は乱数 h $(0 < h < q-1)$を発生する．
step (3-2)　A は次の式によって，s を計算する，$0 < s < q$ である．もし $s = 0$ ならば，step (3-1) にもどる．

$$(x_1, x_2) = hP \tag{38}$$
$$s = x_1 \bmod q \tag{39}$$

step (3-3)　$h^{-1} \bmod q$を計算し，次の式によって t を計算する．

$$t = h^{-1}(H(m) + d_a s) \bmod q \tag{40}$$

ここで，$H(m)$ はメッセージ m のハッシュ値である．もし $t = 0$ ならば，step (3-1) にもどる．
step (3-4)　メッセージ m のディジタル署名文(s,t)を受信者 B に送る．
ディジタル署名文の認証：ディジタル署名文(s,t)は送信者 A が署名したことを，受信者 B が以下のように認証する．
step (4-1)　B は次の式によって，wを計算する．

$$w = t^{-1} \bmod q \tag{41}$$

step (4-2)　B はメッセージ m のハッシュ値 $H(m)$ を計算する．
step (4-3)　B は次の式によって，u_1, u_2を計算する．

$$u_1 = H(m)w \bmod q \tag{42}$$
$$u_2 = sw \bmod q \tag{43}$$

step (4-4)　B は次の式によって，vを計算する．

$$u_1P + u_2Q_a = (x_0, y_0) \tag{44}$$
$$v = x_0 \bmod q \tag{45}$$

step (4-5)　もし $v = s$ ならば，メッセージは A が送ったことが確認できる．

ここで，メッセージ m のディジタル署名文(s,t)を本当に A が送ったのであれば，式 (44) において

$$\begin{aligned}(x_0, y_0) &= u_1P + u_2Q_a \\ &= (H(m)t^{-1} \bmod q)P + (st^{-1} \bmod q)d_aP \\ &= [(H(m) + sd_a)t^{-1} \bmod q]P \\ &= hP \\ &= (x_1, x_2)\end{aligned}$$

となるから，$x_0 = x_1$が成り立つ．故に $v = s$ が成り立つ．

5　まとめ

楕円曲線暗号は，公開鍵暗号系として最も注目されている暗号である．本論文では離散対数生成器に基づく楕円曲線暗号系を提案した．提案した暗号系に関連して楕円曲線理論，離散対数問題と楕円曲線上の離散対数問題，離散対数生成器および ElGamal 暗号系列を説明した．提案した暗号系の安全性は楕円曲線上の離散対数問題に依存する．いままで楕円曲線上の離散対数問題に対して準指数時間となるアルゴリズムは知られていない．この意味で，提案する暗号系は安全である．

参考文献

[1] W. Differ and M.E. Hellman.“New directions in cryptography, ” IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[2] N. Koblitz, “Algebraic aspects of cryptosystem, ” Springer-Verlag, 1998.

[3] T. ElGamal, “A public key sryptosystem and a signature scheme base on discrete logarithms , ” IEEE Trans. Inform. Theory, vol. IT-31, no. 4, pp. 469-472, 1985.

[4] N. Koblitz, “Elliptic curve cryptosystems, ” Mathematics of Computing, vol. 48, pp. 203-209, 1987.

[5] A.J. Menezes and S.A. Vanstone , “Elliptic cryptosystem and their implementation ,” Journal of Cryptology, no. 6, pp. 209-224, 1993.

[6] M. Blum and S. Micali, “How to generate cryptographically strong sequence of pseudo-random bits, ” SIAM Jounal on Computing, vol. 13, pp. 850-854, 1984.

[7] D.R. Stinson, (桜井　幸一監訳) “暗号理論の基礎, ” 共立出版, 1996.